DETAILED ACTION

1. In response to amendment filed on 17 December 2007 and Examiner Initiated Interview on 6 March 2008. Claims 4, 5, 7-11, 13, 14, 16, 18, and 19 have been amended. Claims 1-3, 15, 17, and 20 have been canceled.

2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment was authorized by attorney of record George Sai-Halasz, PhD in phone interview on 6 March 2008.

Response to Arguments

3 Applicant's arguments filed 17 December 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

4. Claims 4-14, 16, 18, and 19, are allowed.

Conclusion

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2134
7 March 2008

Examiner's Amendment

This listing of the claims will replace all prior versions and listings of the claims in the application:

Listing of Claims:

1-3 (canceled)

4. (Currently Amended) A method for secure unlocking of a door based on a shared secret key, comprising the steps of:

providing a portable computing device, wherein the computing device is equipped with a memory, and the memory holds ~~a first copy of the~~ shared secret ~~key~~ keys with matching door identifiers, and a first ~~standard~~ certificate, wherein the computing device is adapted for performing operations with shared secret keys and ~~standard~~ certificates, and wherein the computing device is ~~also having means~~ adapted for communicating with the door;

~~communicating by~~ the computing device communicating to the door a device identifier;

the door makes a decision to issue a challenge to the computing device, ~~issuing a challenge by the door to the computing device,~~ wherein the challenge is issued only on randomly selected occasions;

the computing device responding to the challenge by ~~the computing device by~~ demonstrating possession of a private key [[part]] of the first ~~standard~~ certificate;

~~responding by~~ after a successful response to a challenge and after receipt of computing device identifier when a challenge decision is not made the door responding with a door identifier and with [[a]] an encrypted message, wherein the message is encrypted with ~~a second copy of~~ the shared secret key, and wherein using ~~the second copy of~~ the shared secret key for

encrypting the message resulted from recognizing the device identifier communicated by the computing device;

~~responding by~~ the computing device responding with a signal attesting decryption of the message, wherein the message has been decrypted in the computing device by ~~the first copy of~~ the shared secret key, and wherein using ~~the first copy of~~ the shared secret key for decrypting the message resulted from recognizing the door identifier transmitted by the door; and

~~unlocking~~ the door unlocking upon recognizing validity of the signal attesting decryption of the message.

5. (Currently Amended) The method of claim 4, wherein the device identifier is a hash code of the first ~~standard~~ certificate.

6. (original) The method of claim 4, wherein the door identifier is a simple identifier and it is sent without encryption.

7. (Currently Amended) The method of claim 4, wherein the door has a second ~~standard~~ certificate, and the door identifier is a hash code of the second ~~standard~~ certificate.

8. (Currently Amended) The method of claim 4, wherein the shared secret key is generated by the door and communicated with the computing device in private using a public key [[part]] of the first ~~standard~~ certificate.

9. (Currently Amended) The method of claim 4, wherein the private key [[part]] of the first ~~standard~~ certificate is encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device, and wherein the computing device is provided with a biometric device, and wherein the step of responding to the challenge further comprise the steps of: taking a biometric reading of a user of the computing device; generating a second biometric key using the biometric reading; and decrypting the encrypted private key [[part]] of the first ~~standard~~ certificate using the second biometric key, whereby if the first and second biometric keys are identical the decrypting using the second biometric key is successful, and the challenge can be successfully responded.

10. (Currently Amended) A security system for controlling access, comprising:

a [[first]] plurality of doors and a ~~second~~ plurality of portable computing devices for opening the plurality of doors[[,]];

wherein each computing device is equipped with a memory~~, wherein any one of the computing devices~~ that holds ~~in its memory~~ a unique first ~~standard~~ certificate, ~~and wherein the any one computing device further holds in its memory~~ door identifiers for all the doors out of the ~~first~~ plurality of doors that the ~~any one~~ computing device is permitted to open, and ~~wherein each of the door identifier is uniquely linked to a first copy of a~~ shared secret keys that match each door identifier of the plurality of doors that the computing device is permitted to open; [[key,]]

wherein any one of the doors possesses a matching shared secret key ~~information~~ for each ~~one of those~~ computing device ~~devices out of the second plurality of computing devices~~ that is [[are]] permitted to open the ~~any one~~ door,

wherein the matching information comprises a device identifier, wherein the device identifier is linked to a public key [[part]] of the unique first ~~standard~~ certificate and ~~to a second copy of~~ the shared secret key, and wherein the ~~first~~ plurality of doors and the ~~second~~ plurality of computing devices have means for communicating between any device and any door[[,]] and;

wherein the any one of the plurality of doors ~~door~~ is adapted to recognize the device identifier, and further adapted to use the matching information to validate identicalness of the ~~first and the second copies of the~~ shared secret key, and to issue a challenge on randomly selected occasions to any computing device, ~~the unique first standard certificate~~ using the public key [[part]] of the unique first ~~standard~~ certificate.

11. (Currently Amended) The security system of claim 10, wherein the device identifier is a hash code of the unique first ~~standard~~ certificate.

12. (original) The security system of claim 10, wherein the door identifier is a simple identifier and it is communicated without encryption.

13. (Currently Amended) The security system of claim 10, wherein the any one door further possesses a unique second ~~standard~~ certificate.

14. (Currently Amended) The security system of claim 13, wherein the door identifier is a hash code of the unique second ~~standard~~ certificate.

15. (canceled)

16. (Currently Amended) The security system of claim 10, wherein the unique first ~~standard~~ certificate is having a private key [[part]] and the private key [[part]] is being encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device, wherein the any one computing device is further comprising a biometric device, wherein the any one computing device is further comprising a biometric device, wherein the biometric device is capable of generating a second biometric key, wherein the second biometric key belongs to a user of the any one computing device, and wherein the second biometric key is used to decrypt the private key [[part]] of the unique first ~~standard~~ certificate.

17. (canceled)

18. (Currently Amended) The security system of claim 10, wherein the challenge by the any one door is successfully responded by demonstrating possession of a private key [[part]] of the unique first ~~standard~~ certificate.

19. (Currently Amended) The security system of claim 10, wherein the any one door is further adapted to generate a shared secret key and communicate the shared key in private by using the public key [[part]] of the unique first ~~standard~~ certificate.

20. (canceled)

/ELLEN TRAN/
Primary Examiner, Art Unit 2134